IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

JENNIFER KILKUS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

THE CORPORATION OF MERCER UNIVERSITY,

Defendant.

Case No.

Complaint – Class Action

Demand for Jury Trial Enclosed

INTRODUCTION

1. This case arises from a data breach. *See* Notice of Data Breach (Exhibit 1). Defendant The Corporation of Mercer University is a sophisticated institution with an endowment of more than $452 million.[1] It collects and stores vast amounts of highly sensitive data about its students and employees—including personally identifiable information (PII) such as names, social security numbers, and driver's license numbers. Mercer's students and employees have no choice but to trust Mercer to keep their data secure.

2. An unauthorized third-party successfully hacked Mercer's systems and absconded with the PII of 93,512 victims. Criminals can now sell

[1] *Facts and Figures*, MERCER UNIVERSITY (accessed June 1, 2023), https://www.mercer.edu/about-mercer/facts-and-figures/.

the victims' data on the black market for the purpose of stealing their identities. None of this would have occurred if Mercer had implemented reasonable data security measures.

3. Plaintiff Dr. Jennifer Kilkus is a victim of the data breach. She brings this action on behalf of herself and all others similarly situated, seeking damages for the injuries that Mercer's negligence has caused, as well as injunctive relief to ensure that the data that Mercer continues to store will be protected by reasonable data security practices going forward.

PARTIES

4. Plaintiff Jennifer Kilkus, PhD, ABPP is an Assistant Clinical Professor at the Yale School of Medicine who resides in Connecticut. Dr. Kilkus taught a course at Mercer University in 2016 and 2018.

5. Defendant The Corporation of Mercer University is a corporation with its principal place of business located in Georgia.

6. On information and belief, Mercer made the decisions giving rise to the data breach from its Georgia headquarters—including decisions regarding its data security policy and procedures, as well as its response to the data breach.

JURISDICTION AND VENUE

7. The Court has personal jurisdiction over Mercer because Mercer's principal place of business is located in Georgia.

8. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d)(2) because: at least one member of the proposed Class, including Dr.

Kilkus, is a citizen of a state different from that of Mercer; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members; and none of the exceptions under that subsection apply to this action.

9. Venue is proper because a substantial part of the events and omissions giving rise to the claims occurred in the Northern District of Georgia, including from Mercer's Atlanta campus.

FACTUAL ALLEGATIONS

A. Mercer allowed Dr. Kilkus's data to be stolen.

10. Earlier this year, criminals hacked Mercer's computer systems. The criminals accessed files on Mercer's systems between February 12, 2023 and February 24, 2023.

11. The criminals accessed files that contained PII of Dr. Kilkus and the Class. This PII included the victims' names, social security numbers, and/or driver's license numbers.

12. Mercer discovered the hack on April 5, 2023. However, Mercer did not learn that PII was exposed in the data breach until April 30, 2023. If Mercer had exercised reasonable diligence in its investigation, it would have learned far sooner that PII had been exposed.

13. Mercer did not begin notifying victims of the data breach until approximately May 19, 2023—a delay of about three months. This delay was unreasonable under the circumstances and prevented Dr. Kilkus and the

Class from taking action sooner to protect themselves from identity theft, thus increasing their already substantial risk of harm.

14. Mercer offered victims of the data breach with one year of "identity theft protection services." Exhibit 1. These services include monitoring for fraud, identity restoration, and up to $1 million of identity theft insurance. Therefore, Mercer itself understands that: (1) class members are at an imminent and substantial risk of identity theft; (2) the risk of identity theft is ongoing and will continue for multiple years; and (3) identity theft can cause at least $1 million in damages.

15. However, the identity theft monitoring services that Mercer offered are inadequate. They are available only for two years, despite that the risk of identity theft often persists for far longer. And the overall benefits do not adequately address the severity of the risk of harm faced by Plaintiff and the Class.

16. Mercer also provided class members with instructions on reviewing their accounts for signs of fraud or identity theft, placing fraud alerts on their credit reports, and reporting identity theft to the police or FTC. This further demonstrates Mercer's knowledge of the substantial risk of identity theft faced by class members.

B. The data breach was highly foreseeable, yet Mercer failed to take reasonable precautions.

17. Given the type of data that Mercer collected and stored, it was highly foreseeable that bad actors would attempt to access it without permission.

18. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id.* at 855.

19. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

20. Because Mercer collected and stored identifying and financial information that is very valuable to criminals, it was highly foreseeable that a bad actor would attempt to access that data without permission.

21. Mercer frequently collects and stores personally identifying and financial information. Therefore, the burden (if any) of implementing reasonable data security practices is minimal in comparison to the substantial and highly foreseeable risk of harm.

22. Moreover, Mercer is well aware that its role as a university makes it an attractive target for hackers. The letter that Mercer sent to victims of the data breach even acknowledges that "hundreds of higher educational institutions" have been targeted by hackers. Exhibit 1. Despite its knowledge of the highly foreseeable risk that it, too, would be targeted by hackers, Mercer failed to exercise reasonable care.

23. On information and belief, Mercer failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;
b. Locking, encrypting and limiting access to computers and files containing sensitive information;
c. Implementing guidelines for maintaining and communicating sensitive data;
d. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and
e. Providing focused cybersecurity awareness training programs for employees.

24. In addition, the FTC has noted the need to factor data security into all business decision-making. *Start With Security, A Guide for Business*, FTC (accessed June 9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4)

limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

25. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available

security measures to limit access between instore networks . . .”). These orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

26. On information and belief, Defendant’s use of outdated and insecure computer systems and software that are easy to hack, and their failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and tens of thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

27. Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security, which allowed class members’ data to be accessed and stolen by criminals.

C. Dr. Kilkus’s information was exposed in the data breach, which caused her to suffer concrete injuries.

28. Plaintiff Dr. Jennifer Kilkus is a former Mercer employee. She entrusted Mercer with her personally identifying and financial information as a condition of her employment.

29. Dr. Kilkus received a data breach notification informing her that her PII had been accessed in the data breach, including her name, social security number, and/or driver’s license number.

30. Dr. Kilkus typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

31. As a result of the data breach, Dr. Kilkus suffered a severe privacy injury. Dr. Kilkus, like any reasonable person, strongly prefers to keep her PII private. She shares her PII only insofar as necessary—and only to specific people or entities, for limited purposes, on the understanding that the recipient will take reasonable steps to keep her PII secure. Now that criminals have obtained access to Dr. Kilkus's PII, any person can now purchase highly sensitive information about Dr. Kilkus on the black market. Dr. Kilkus has thus lost control of highly sensitive information concerning her person. Mercer's negligence thus caused Dr. Kilkus and the Class to suffer a legally cognizable privacy injury.

32. Plaintiff also suffered a loss of time, as she has spent and continues to spend a considerable amount of time on issues related to this Data Breach, including by monitoring her accounts, obtaining credit monitoring, and apprising herself of the situation. This is time that was lost and unproductive and took away from other activities and duties.

33. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant—which was compromised in and as a result of the data breach.

34. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the data breach and has anxiety and increased concerns for the loss of her privacy.

35. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of criminals.

36. Defendant continue to maintain Plaintiff's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff would not have entrusted her PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

37. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the data breach. As a result of the data breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

38. Because their personally identifying and financial information has been accessed by criminals, Plaintiff and the Class have suffered concrete and ongoing injuries.

39. Plaintiff and the Class are at an imminent and substantial risk of identity theft.

40. According to experts, one out of four data breach notification recipients become a victim of identity fraud. *Study Shows One in Four Who*

Receive Data Breach Letter Become Fraud Victims, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

41. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

42. The value of Plaintiff's and the proposed Class PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

43. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

44. One such example of criminals using PII for profit is the development of "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in

various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://bit.ly/3Qj2eJd.

45. Cyber-criminals can cross-reference two sources of PII to marry unregulated or partial data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete "Fullz" dossiers on individuals.

46. The development of "Fullz" packages means that stolen PHI from the data breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the data breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is likely what is already happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury,

to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the data breach.

47. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

48. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

49. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

50. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

51. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To

protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

52. Moreover, the breach has diminished the value of Plaintiff and the Class's personal information.

53. The FTC has recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

54. Since it was included in the breach, Plaintiff and the Class's information has already been accessed by criminals, which decreases its value in the marketplace.

55. Therefore, the value of Plaintiff and the Class's personal information was reduced by the data breach.

56. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

57. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

58. None of those injuries would have occurred if Defendant had implemented reasonable data security practices.

CLASS ACTION ALLEGATIONS

59. Pursuant to FED. R. CIV. P. 23(b)(2) and (b)(3), Plaintiff seeks certification of a Class defined as follows:

> All individuals whose personally identifiable information was compromised in connection with the data breach affecting Mercer University from approximately February 12, 2023 to February 24, 2023, including all those who received notice of the data breach.

60. Excluded from the Class are: (a) Defendant and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

61. *Ascertainability*. The Class can be readily identified through Mercer's records, which is demonstrated by the fact that many class members

have already been identified and sent notice letters regarding the data breach.

62. *Numerosity*. Mercer has represented to the Maine Attorney General that 93,512 individuals had their information exposed in the data breach. Therefore, the Class is so numerous that individual joinder is impracticable.

63. *Typicality*. Plaintiff's claims are typical of the Class she seeks to represent. Like all class members, Plaintiff's PII was exposed in the data breach as a result of Defendant's failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

64. *Adequacy of Class Representative*. Plaintiff will fairly and adequately protect the interests of the Class. She is aware of her fiduciary duties to absent class members and is determined to faithfully discharge her responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

65. *Adequacy of Counsel*. In addition, Plaintiff has retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiff's counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

66. *Commonality and Predominance.* This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PII;

c. Whether Defendant breached its contractual promises to safeguard Plaintiff and the Class's PII;

d. Whether Defendant knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff and the Class's PII from unauthorized release and disclosure;

g. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

h. Whether Defendant is liable for negligence, gross negligence, or recklessness;

i. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

j. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

k. What the proper measure of damages is; and

l. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

67. *Superiority and Manageability*. A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

68. *Injunctive or Declaratory Relief*. In addition, Defendant acted or failed to act on grounds that apply generally to the Class, such that final injunctive or declaratory relief as to any one class member is appropriate as to all class members.

CAUSES OF ACTION

Count 1: Negligence

69. Plaintiff incorporates paragraphs 1–## by reference.

70. It was highly foreseeable that a failure to reasonably safeguard Plaintiff and the Class's PII would lead to a data breach. Plaintiff and the Class are members of a well-defined, foreseeable, and probable group of individuals whom Mercer knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and the Class's personal and financial

information in the conduct of its business, and Defendant retained that information. Moreover, Defendant was well aware that it was part of an industry that is frequently targeted by hackers, as well as that the PII it was collecting and storing made it a prime target for criminal hackers.

71. Therefore, Mercer owed a duty to anticipate the harm of a criminal data breach and exercise reasonable care to guard against it.

72. Mercer breached its duty of reasonable care on many levels, including but not limited to, its failure:

a. To use its heightened cybersecurity expertise to avoid causing the data breach, including by adhering to the recommendations in its cybersecurity white papers;
b. To implement industry-standard security procedures sufficient to reasonably protect the information from the data breach;
c. To implement industry-standard security procedures for detecting and responding to an actual or attempted data breach;
d. To reasonably train its employees on data security procedures; and
e. To reasonably supervise its agents, contractors, vendors, and suppliers who were charged with handling and securing the PII of Plaintiff and the Class.

73. Mercer breach of its duty of care was willful or reckless. Mercer was well aware of the cybersecurity risks that result from unreasonable data security practices, yet it consciously disregarded those risks without adequate justification.

74. Mercer's recklessness or negligence directly and foreseeably caused Plaintiff and the Class's injuries, including, without limitation, theft of their PII by criminals, improper disclosure of their PII, loss of privacy, lost

value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach. But-for Mercer's negligence, those injuries would not have occurred.

Count 2: Negligence Per Se

75. Plaintiff incorporates paragraphs 1–## by reference.

76. Pursuant to the FTC Act, 15 U.S.C. § 45, Mercer had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

77. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class's sensitive PII.

78. Mercer violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Mercer's conduct was particularly unreasonable given the nature and amount of PII that Mercer had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

79. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

80. Mercer had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

81. Mercer breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

82. Mercer's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

83. Mercer's failure to adhere to the standard of care under Section 5 of the FTC Act directly and foreseeably caused Plaintiff and the Class's injuries, including, without limitation, theft of their PII by criminals, improper disclosure of their PII, loss of privacy, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach. But-for Mercer's negligence, those injuries would not have occurred.

Count 3: Breach of Contract

84. Plaintiff incorporates paragraphs 1–## by reference.

85. Plaintiff and the Class entered employment contracts with Mercer, in which they provided services in exchange for consideration.

86. As a condition of those contracts, Mercer required Plaintiff and the Class to provide it with their PII.

87. Implicit in the parties' agreement was that Defendant would reasonably safeguard Plaintiff and the Class's PII.

88. Mercer knew that its employees reasonably expected that it would take reasonable precautions to safeguard the PII they provided in the course of their employment.

89. Mercer also owed Plaintiff and the Class an implied duty of good faith and fair dealing. Under this implied covenant, Mercer was obligated to reasonably safeguard the PII that it required Plaintiff and the Class to provide as a condition of their employment.

90. Mercer failed to reasonably safeguard Plaintiff and the Class's PII on many levels, including but not limited to, its failure:

f. To use its heightened cybersecurity expertise to avoid causing the data breach, including by adhering to the recommendations in its cybersecurity white papers;

g. To implement industry-standard security procedures sufficient to reasonably protect the information from the data breach;

h. To implement industry-standard security procedures for detecting and responding to an actual or attempted data breach;

i. To reasonably train its employees on data security procedures; and

j. To reasonably supervise its agents, contractors, vendors, and suppliers who were charged with handling and securing the PII of Plaintiff and the Class.

91. Plaintiff and the Class have performed as required under the contract and satisfied any conditions precedent to filing suit.

92. As a direct and foreseeable result of Mercer's breach of contract, Plaintiff and the Class suffered damages, including, without limitation, theft of their PII by criminals, improper disclosure of their PII, loss of privacy, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach. But-for Mercer's breach of contract, those injuries would not have occurred.

Count 4: Unjust Enrichment

(In the Alternative to Count 3)

93. Plaintiff incorporates paragraphs 1–## by reference.

94. This claim is asserted in the alternative to Count 3.

95. Mercer required Plaintiff and the Class to provide their PII as a condition of employment.

96. Plaintiff and the Class conferred a benefit on Mercer in the form of the services they provided within the scope of their employment. The value of these services priced-in the cost of data security, as Plaintiff and the Class reasonably expected that Mercer would implement reasonable safeguards to protect the PII that it required them to hand-over. If Mercer had revealed that it would not reasonably safeguard Plaintiff and the Class's PII, they would not have accepted employment at the rates that they did.

97. Mercer knew of the benefits conferred on it by Plaintiff and the Class.

98. Mercer failed to implement reasonable data security measures. This allowed Mercer to cut costs and pocket the portion of Plaintiff's wages that had priced-in the expectation of reasonable data security safeguards.

99. Under principals of equity and good conscience, Mercer should not be permitted to retain the full value of Plaintiff and the Class's services and their PII because Mercer failed to adequately protect their PII. Plaintiff and the Class would not have provided their PII to Mercer if they had known Mercer would not adequately protect their PII.

100. Plaintiff and the Class lack an adequate remedy at law.

101. Therefore, Mercer should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds it received due to its misconduct.

PRAYER FOR RELIEF

102. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;
b. Appointment of the undersigned counsel as class counsel;
c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;
d. Restitution or disgorgement of all ill-gotten gains; and
e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

103. Plaintiff demands a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Matthew R. Wilson*

Matthew R. Wilson (871480)
Jared W. Connors (*pro hac vice* to be filed)
MEYER WILSON CO., LPA
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066
mwilson@meyerwilson.com
jconnors@meyerwilson.com

Samuel J. Strauss (*pro hac vice* to be filed)
Raina Borrelli (*pro hac vice* to be filed)
TURKE & STRAUSS LLP
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class